Freeform Search

Database: US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Term: L28 not l25

Display: 10 **Documents in Display Format:** TI **Starting with Number** 1

Generate: ○ **Hit List** ◉ **Hit Count** ○ **Side by Side** ○ **Image**

Search Clear Interrupt

Search History

DATE: Thursday, November 03, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
L29	L28 not l25	0	L29
L28	L24 and (("black$ box" or "black-box" or "black box") same (decrypt$ or encrypt$ or crypto?$)) and @ad<=19990327	3	L28
L27	L26 not l25	1	L27
L26	L24 and (black$ same (decrypt$ or encrypt$ or crypto?$)) and @ad<=19990327	4	L26
L25	L24 and (black$ with (decrypt$ or encrypt$ or crypto?$)) and @ad<=19990327	3	L25
L24	L6 or l12	273	L24
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L23	L18 and (decrypt$ same licens$)	1	L23
L22	L18 and decrypt$	1	L22
L21	L18 and black$	1	L21
L20	L18 and (black$ same encrypt$)	0	L20
L19	L18 and (black$ same decrypt$)	0	L19
L18	6343280.pn.	1	L18

DB=EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR

L17	L14 and ibm$	0	L17
L16	L14 and baratti$	0	L16
L15	L14 and baratti	0	L15
L14	9903798$	17	L14

DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR

L13	L12 and black$	3	L13
L12	6226618.pn. or 6343280.pn. or 6574612.pn. or 6073124.pn. or 5715403.pn. or 6006332.pn. or 6112181.pn.	7	L12
L11	L10 and black$	2	L11
L10	6226618.pn. or 6343280.pn. or 6574612.pn. or 6073124.pn. or 5715403.pn.	5	L10
L9	6226618.pn. or 6343280.pn. or 6574612.pn. or 6073124.pn. or 6715403.pn.	5	L9

DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR

L8	L6 and drm$ and (license adj serv$)	3	L8
L7	L6 and drm and (licenser adj serv?)	0	L7
L6	L3 or L5	268	L6
L5	(5864620 | 4905163 | 5191573 | 5606617 | 5915025 | 5787413 | 5751805 | 5541991 | 6009543 | 5999629 | 5355302 | 4218582 | 6343280 | 4782529 | 5604804 | 5982892 | 5588060 | 5745574 | 5754646 | 4879747 | 4926479 | 5592664 | 5319705 | 5923882 | 5657473 | 4825306 | 5758069 | 5224163 | 4944006 | 5005200 | 5706347 | 4463387 | 5224166 | 5636139 | 5130792 | 5889860 | 5757914 | 5892900 | 5347580 | 4924378 | 5537475 | 5222133 | 4405829 | 5991399 | 5557541 | 5220604 | 5530752 | 5652793 | 5261002 | 4868687 | 4757534 | 5497421 | 5260788 | 5675734 | 5671412 | 4424414 | 5710887 | 5646992 | 5745879 | 4888798 | 4995082 | 5276901 | 5412717 | 5371794 | 5646998 | 4200770 | 4272810 | 5765152 | 5905860 | 5315658 | 5509071 | 5519778 | 4803725 | 4868877 | 4731840 | 5917912 | 5606609 | 5214702 | 5790664 | 5657388 | 4528643 | 5159634 | 4465901 | 4878246 | 4809327 | 5673316 | 6018712 | 6047242 | 5420927 | 5666420 | 5581479 | 5369705 | 5796841)![PN]	190	L5
L4	('WO 200008909A'| 'US 6343280B'| '6574612'| '6343280'| '6226618'| '6574609'| 'GB 2346989A')[PN]	7	L4
L3	('WO 200008909A'| 'US 6343280B'| '6574612'| '6343280'| '6226618'| '6574609'| 'GB 2346989A')[URPN]	78	L3
L2	6226618.pn. or 6343280.pn. or 6574612.pn. or 6574609.pn.	7	L2

DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR

L1	6343290.pn.	1	L1

END OF SEARCH HISTORY

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

End of Result Set

Generate Collection Print

L27: Entry 1 of 1 File: USPT Nov 9, 1993

US-PAT-NO: 5261002
DOCUMENT-IDENTIFIER: US 5261002 A

TITLE: Method of issuance and revocation of certificates of authenticity used in public key networks and other systems

DATE-ISSUED: November 9, 1993

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Perlman; Radia J.	Acton	MA		
Kaufman; Charles W.	Northborough	MA		

US-CL-CURRENT: 380/30; 713/156, 713/158

ABSTRACT:

A technique for issuing and revoking user certificates of authenticity in a public key cryptography system, wherein certificates do not need expiration dates, and the inconvenience and overhead associated with routine certificate renewals are minimized or avoided entirely. A Certification Authority issues certificates as required, and issues a blacklist having a start date, an expiration date, and an entry for every invalid certificate issued after the start date. Users assume that every certificate issued prior to the blacklist start date is invalid, and that invalid certificates issued after the start date will be included in the current blacklist. A new blacklist is issued prior to expiration of the current one, and the blacklist start date is changed only when the blacklist becomes unmanageably long.

18 Claims, 2 Drawing figures
Exemplary Claim Number: 7
Number of Drawing Sheets: 2

Previous Doc Next Doc Go to Doc#

L12: Entry 2 of 3 File: USPT Jan 29, 2002

US-PAT-NO: 6343280
DOCUMENT-IDENTIFIER: US 6343280 B1

TITLE: Distributed execution software license server

DATE-ISSUED: January 29, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Clark; Jonathan	Austin	TX	78749	

APPL-NO: 09/212373 [PALM]
DATE FILED: December 15, 1998

INT-CL: [07] H04 L 9/00

US-CL-ISSUED: 705/55; 705/51
US-CL-CURRENT: 705/55; 705/51

FIELD-OF-SEARCH: 705/1, 705/50-59, 380/201, 380/202

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4465901	August 1984	Best	713/190
☐	4888798	December 1989	Earnest	705/54
☐	4924378	May 1990	Hershey et al.	364/200
☐	5222133	June 1993	Chou et al.	705/55
☐	5530752	June 1996	Rubin	705/59
☐	5541991	July 1996	Benson et al.	713/202
☐	5606609	February 1997	Houser et al.	380/4
☐	5652793	July 1997	Priem et al.	705/56
☐	5657388	August 1997	Weiss	380/23
☐	5657473	August 1997	Killean et al.	711/163
☐	5745879	April 1998	Wyman	705/1
☐	5751805	May 1998	Otsuki et al.	705/54

☐	5754646	May 1998	Williams et al.	705/55
☐	5757914	May 1998	McMainis	380/23
☐	5758069	May 1998	Olsen	395/187.01
☐	5790664	August 1998	Coley et al.	380/4
☐	5905860	May 1999	Olsen et al.	395/187.01
☐	5923882	July 1999	Ho et al.	395/709
☐	6009543	December 1999	Shavit	714/200
☐	6018712	January 2000	Pactong	705/1

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	CLASS
WO 9013865	November 1990	WO	

OTHER PUBLICATIONS

Definition of "executable file" at http://www.webopedia.com, Jul. 3, 2001.

ART-UNIT: 2162

PRIMARY-EXAMINER: Stamber; Eric W.

ASSISTANT-EXAMINER: Champagne; Donald L.

ATTY-AGENT-FIRM: Lee; Larry Mason

ABSTRACT:

A method of protecting an executable image from unlicensed use is provided by remote execution of sequences of microprocessor instructions. Means of selecting sequences of instructions that execute infrequently and provide a high level of security against reverse engineering is provided. Selection means includes run-time profiling of an executable running under normal conditions. The selected sequences of instructions are replaced with instructions that interrupt the normal flow of execution and transfer control to a license server. A client computer executes the modified executable until the replaced sequences interrupt the normal flow of execution and transfer control to a license server. The license server executes the instructions which were replaced in the modified executable upon proper authorization by emulating the client microprocessor.

16 Claims, 18 Drawing figures

Previous Doc Next Doc Go to Doc#

L12: Entry 2 of 3 File: USPT Jan 29, 2002

DOCUMENT-IDENTIFIER: US 6343280 B1
TITLE: Distributed execution software license server

Detailed Description Text (23):
The removal of a single instruction from a computer program typically does not result in a sufficiently complex relationship between inputs and outputs of the execution of the single instruction to permit protection because most computer systems have a small set of instructions that have a limited effect. By watching the inputs and outputs of the operation of a single missing instruction the instruction could be easily guessed, derived, or reverse engineered. For this reason, the instant invention uses a sequence of instructions which when grouped together have a combined effect that is much more complex and difficult to determine. The length of an instruction sequence 298 to be removed from the Original Software 9 and placed on the License Server 4 for remote execution is determined by the process shown in FIG. 7. An instruction sequence 298 can be thought of as a black box having only inputs and outputs. The inputs include any memory or CPU registers that are to be accessed by the execution of the instruction sequence 298. The outputs are any memory or CPU registers that are modified by the execution of the instruction sequence 298. Because the instant invention operates on instruction sequences 298 rather than on individual instructions, information for determining the execution differences (as discussed above) can be stored for an entire instruction sequence, thereby saving memory space and time. By running the program twice and recording the inputs and outputs of each of the instruction sequences 298, differences will result if the Software User 2 operates the software differently on the two runs. These differences are easily identified by matching the inputs of one run with those of another run. A difference is identified when no matches occur or the outputs differ for matched inputs.

L25: Entry 1 of 3 File: USPT Jun 29, 1999

DOCUMENT-IDENTIFIER: US 5917912 A
** See image for Certificate of Correction **
TITLE: System and methods for secure transaction management and electronic rights protection

Application Filing Date (1):
19970108

Detailed Description Text (1742):
Delivery of audit reports through a path of handling may be in part insured by an inverse (return of information) audit method. Many VDE methods have at least two pieces: a portion that manages the process of producing audit information at a user's VDE node; and a portion that subsequently acts on audit data. In an example of the handling of audit information bound for a plurality of auditors, a single container object is received at a clearinghouse (or other auditor). This container may contain (a) certain encrypted audit information that is for the use of the clearinghouse itself, and (b) certain other encrypted audit information bound for other one or more auditor parties. The two sets of information may have the same, overlapping and in part different, or entirely different, information content. Alternatively, the clearinghouse VDE node may be able to work with some or all of the provided audit information. The audit information may be, in part, or whole, in some summary and/or analyzed form further processed at the clearinghouse and/or may be combined with other information to form a, at least in part, derived set of information and inserted into one or more at least in part secure VDE objects to be communicated to said one or more (further) auditor parties. When an audit information container is securely processed at said clearinghouse VDE node by said inverse (return) audit method, the clearinghouse VDE node can create one or more VDE administrative objects for securely carrying audit information to other auditors while separately processing the secure audit information that is specified for use by said clearinghouse. Secure audit processes and credit information distribution between VDE participants normally takes place within the secure VDE "black box," that is processes are securely processed within secure VDE PPE 650 and audit information is securely communicated between the VDE secure subsystems of vDE participants employing VDE secure communication techniques (e.g., public key encryption, and authentication).

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

Generate Collection Print

L25: Entry 1 of 3 File: USPT Jun 29, 1999

US-PAT-NO: 5917912
DOCUMENT-IDENTIFIER: US 5917912 A
**** See image for Certificate of Correction ****

TITLE: System and methods for secure transaction management and electronic rights protection

DATE-ISSUED: June 29, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ginter; Karl L.	Beltsville	MD		
Shear; Victor H.	Bethesda	MD		
Spahn; Francis J.	El Cerrito	CA		
Van Wie; David M.	Sunnyvale	CA		

US-CL-CURRENT: 713/187; 705/40, 713/164, 719/312

ABSTRACT:

The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

58 Claims, 153 Drawing figures
Exemplary Claim Number: 58
Number of Drawing Sheets: 146

Previous Doc Next Doc Go to Doc#

L25: Entry 2 of 3 File: USPT Apr 6, 1999

DOCUMENT-IDENTIFIER: US 5892900 A
** See image for Certificate of Correction **
TITLE: Systems and methods for secure transaction management and electronic rights protection

Application Filing Date (1):
19960830

Detailed Description Text (1975):
Delivery of audit reports through a path of handling may be in part insured by an inverse (return of information) audit method. Many VDE methods have at least two pieces: a portion that manages the process of producing audit information at a user's VDE node; and a portion that subsequently acts on audit data. In an example of the handling of audit information bound for a plurality of auditors, a single container object is received at a clearinghouse (or other auditor). This container may contain (a) certain encrypted audit information that is for the use of the clearinghouse itself, and (b) certain other encrypted audit information bound for other one or more auditor parties. The two sets of information may have the same, overlapping and in part different, or entirely different, information content. Alternatively, the clearinghouse VDE node may be able to work with some or all of the provided audit information. The audit information may be, in part, or whole, in some summary and/or analyzed form further processed at the clearinghouse and/or may be combined with other information to form a, at least in part, derived set of information and inserted into one or more at least in part secure VDE objects to be communicated to said one or more (further) auditor parties. When an audit information container is securely processed at said clearinghouse VDE node by said inverse (return) audit method, the clearinghouse VDE node can create one or more VDE administrative objects for securely carrying audit information to other auditors while separately processing the secure audit information that is specified for use by said clearinghouse. Secure audit processes and credit information distribution between VDE participants normally takes place within the secure VDE "black box," that is processes are securely processed within secure VDE PPE650 and audit information is securely communicated between the VDE secure subsystems of vDE participants employing VDE secure communication techniques (e.g., public key encryption, and authentication).

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

Generate Collection Print

L25: Entry 2 of 3 File: USPT Apr 6, 1999

US-PAT-NO: 5892900
DOCUMENT-IDENTIFIER: US 5892900 A
** See image for Certificate of Correction **

TITLE: Systems and methods for secure transaction management and electronic rights protection

DATE-ISSUED: April 6, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Ginter; Karl L.	Beltsville	MD		
Shear; Victor H.	Bethesda	MD		
Sibert; W. Olin	Lexington	MA		
Spahn; Francis J.	El Cerrito	CA		
Van Wie; David M.	Sunnyvale	CA		

US-CL-CURRENT: 726/26

ABSTRACT:

The present invention provides systems and methods for electronic commerce including secure transaction management and electronic rights protection. Electronic appliances such as computers employed in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Secure subsystems used with such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Secure distributed and other operating system environments and architectures, employing, for example, secure semiconductor processing arrangements that may establish secure, protected environments at each node. These techniques may be used to support an end-to-end electronic information distribution capability that may be used, for example, utilizing the "electronic highway."

220 Claims, 177 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 163

Previous Doc Next Doc Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

End of Result Set

Generate Collection Print

L25: Entry 3 of 3 File: USPT May 15, 1990

DOCUMENT-IDENTIFIER: US 4926479 A
** See image for Certificate of Correction **
TITLE: Multiprover interactive verification system

Application Filing Date (1):
19880429

Detailed Description Text (393):
Conceptually, we would like to have the use of a black box into which the verifier inputs an encrypted history of the communication, the prover inputs its answer to the question and the output which is given to the verifier is the encrypted answer of the prover and the encrypted next question of the verifier. See FIG. 2.

Previous Doc Next Doc Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

End of Result Set

Generate Collection Print

L25: Entry 3 of 3 File: USPT May 15, 1990

US-PAT-NO: 4926479
DOCUMENT-IDENTIFIER: US 4926479 A
**** See image for Certificate of Correction ****

TITLE: Multiprover interactive verification system

DATE-ISSUED: May 15, 1990

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Goldwasser; Shafi	Cambridge	MA		
Kilian; Joseph	Cambridge	MA		
Wigderson; Avi	Jerusalem			IL
Ben-Or; Michael	Jerusalem			IL

US-CL-CURRENT: 713/180; 340/5.74, 705/67

ABSTRACT:

In a multiparty verification system, a prover and a verifier are coupled to rocess respective outputs to provide a system output such as an identification verification. The prover is formed of plural units which share confidential information used to encrypt information carried by the prover. Communication between the prover units is prevented. The first prover unit encrypts the information based on additional information received from the verifier and transfers the encrypted information to the verifier. Subsequently, the verifier obtains from the second prover unit the shared confidential information required to decrypt a subset of the transmitted encrypted information.

20 Claims, 4 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 1

Previous Doc Next Doc Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

End of Result Set

Generate Collection Print

L27: Entry 1 of 1 File: USPT Nov 9, 1993

DOCUMENT-IDENTIFIER: US 5261002 A
TITLE: Method of issuance and revocation of certificates of authenticity used in public key networks and other systems

Abstract Text (1):
A technique for issuing and revoking user certificates of authenticity in a public key cryptography system, wherein certificates do not need expiration dates, and the inconvenience and overhead associated with routine certificate renewals are minimized or avoided entirely. A Certification Authority issues certificates as required, and issues a blacklist having a start date, an expiration date, and an entry for every invalid certificate issued after the start date. Users assume that every certificate issued prior to the blacklist start date is invalid, and that invalid certificates issued after the start date will be included in the current blacklist. A new blacklist is issued prior to expiration of the current one, and the blacklist start date is changed only when the blacklist becomes unmanageably long.

Application Filing Date (1):
19920313

Brief Summary Text (17):
The present invention resides in a method for authenticating users of an information system and, more specifically, users of a public key cryptography system. In the method of the invention, certificates are not required to have an expiration date, so much of the inconvenience of periodic certificate renewals is avoided. A blacklist has a start date and an expiration date, and any certificates issued prior to the start date are automatically considered invalid.

Previous Doc Next Doc Go to Doc#